IN THE UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF PENNSYLVANIA

AMELIA INGRAO and ELISABETH PACANA,	:	CIVIL ACTION NO.
Plaintiffs,	:	Case No: 2:24-cv-1022-JHS
v.	:	
ADDSHOPPERS, INC., NUTRISYSTEM, INC. and VIVINT, INC.	:	
Defendants.	:	

VIVINT, INC.'S SUPPLEMENTAL BRIEF IN SUPPORT OF MOTION TO DISMISS

Plaintiff Elisabeth Pacana cannot establish Article III standing, nor has she stated a claim for relief, for her single count under the Pennsylvania Wiretapping and Electronic Surveillance Control Act ("WESCA") against Vivint, a company that sells home security systems.[1] But Plaintiff admitted in her Complaint that she only "visited" Vivint's website on one occasion; in fact, she affirmatively states that "**she never provided personal information (including her email) to Vivint.**" Complaint at ¶ 66 (emphasis added). Vivint did not collect any highly sensitive personal information or financial information from her use of Vivint's website – because she never provided any such information to Vivint. *Id*. Plaintiff Pacana therefore cannot establish concrete harm for Article III standing or to state a claim under WESCA. *See In re BPS Direct, LLC*, 2023 WL 8458245, at *12 (E.D. Pa. Dec. 5, 2023) ("**We find Website Users who did not disclose highly sensitive personal information such as medical diagnosis information or financial data from banks or credit cards cannot establish concrete harm**.") (emphasis added). Further, the alleged

[1] Plaintiff Ingrao does not assert a claim against Vivint.

capture of her single "visit" to Vivint's website does not constitute "contents of a communication" to satisfy WESCA.

Additionally, Plaintiff consented to collection of data from her use of Vivint's website, because Vivint's privacy policy expressly informed users of this activity and, even if she failed to read the privacy policy, "prior consent" under WESCA does not require "actual knowledge." *Popa v. Harriet Carter Gifts, Inc.*, 52 F.4th 121, 125 (3d Cir. 2022). Plaintiff also impliedly consented by the very act of seeking out and choosing to use Vivint's website: "Reasonable people understand that what they do on the Internet is not completely private. How could it be?" *Farst v. AutoZone, Inc.*, 2023 WL 7179807, at *4 (M.D. Pa. Nov. 1, 2023) (citations omitted). Plaintiff had no reasonable expectation of privacy in her visit to Vivint's website, any more than she would if she visited a brick and mortar retail store and a clerk, or even a surveillance camera, observed her browsing activity in the store.

For these reasons, as well as those set forth in Vivint's previously submitted briefs supporting its Motion to Dismiss and in oral arguments before this Court, Plaintiff's Complaint should be dismissed in its entirety.

I. Plaintiff failed to state a concrete injury necessary for Article III standing or a WESCA claim.

In her Complaint, in her briefing, and during oral argument, Plaintiff only generically refers to the "harm" she allegedly sustained, instead focusing on theoretical harm that she *could have* sustained and the *capabilities* of AddShopper's data technology – ***not the information actually collected from her visit to Vivint's website***. But crucially, and fatal to her claims, she merely alleges that she "visited" Vivint's website on a single date, and she fails to specify any personal information whatsoever that was captured from that visit. Plaintiff's broad allegations of *theoretical harm* and what the technology *could do* are insufficient for Article III standing. Further,

the Article III analysis on her WESCA claim against Vivint must focus on what alleged harm was caused to her *by Vivint* – not from other Defendants. Plaintiff cannot satisfy *any* of these requirements.

"To establish injury in fact, a plaintiff must show that he or she suffered an invasion of a legally protected interest that is concrete and particularized and actual or imminent, not conjectural or hypothetical." *Spokeo, Inc. v. Robins*, 578 U.S. 330, 338 (2016). "For an injury to be particularized, it must affect the plaintiff in a ***personal and individual way***." *Id*. (emphasis added). A concrete injury "must actually exist," and be "real, and not abstract." *Id.* at 340. "Even if a plaintiff alleges a statutory violation… Article III standing still 'requires a concrete injury[.]'" *Cook v. GameStop, Inc.*, 689 F. Supp. 3d 58, 63 (W.D. Pa. 2023) (citing *TransUnion LLC v. Ramirez*, 549 U.S. 413, 424 (2021)).

In her Complaint, Plaintiff specifically states that she only "visited" Vivint's website one time, and she did not provide any personal information, including her email address, to Vivint. *See* Complaint at ¶66. She never received an email from Vivint. She never purchased a product from Vivint. Rather, Plaintiff alleges that at some unspecified time after she visited the website of *another* company, she received an email *from that company*. *Id*. at ¶ 63. Plaintiff Pacana alleges that she later discovered that "she had been tracked ***by at least a dozen companies for several years***." *Id*. at ¶¶ 63, 66 (emphasis added). Plaintiff cannot and does not allege that Vivint captured or shared her email address – because she admittedly never gave it to Vivint. *Id.* Indeed, Vivint could not have captured her name, email address, personal or sensitive information, financial information, or any information for which she could have a reasonable expectation of privacy or that caused her any actual harm. Any such information collected concerning Plaintiff would necessarily have come from the "at least a dozen" other companies that allegedly tracked her "for

several years" – ***but not from Vivint***. *Id*.

It is undisputed that Vivint never received any purported benefit from Ms. Pacana's visit to its website. She did not purchase any product. She did not even receive an email from Vivint. She has not alleged that Vivint marketed to her in any way. Plaintiff's theory of harm is merely hypothetical.

Plaintiff cannot show that Vivint harmed her in a "***personal and individual way,***" or that she sustained a concrete injury that "actually exist[s]" due to Vivint's conduct. At most, she has only pleaded "conjectural or hypothetical" or "abstract" theories – which are not sufficient to establish standing or concrete harm as to Vivint. *Spokeo*, 578 U.S. at 338. "Eavesdropping on communications that do not involve personal information, personally identifiable information, or information over which a party has a reasonable expectation of privacy does not amount to a concrete injury." *Massie v. Gen. Motors LLC*, 2022 WL 534468, at *5 (D. Del. Feb. 17, 2022); *see also TransUnion*, 594 U.S. at 424; *Cook*, 689 F. Supp. 3d at 65.

The reasoning and holding of *In re BPS Direct, LLC*, 2023 WL 8458245, at *12 (E.D. Pa. Dec. 5, 2023), with facts almost identical to this case, is instructive. The plaintiffs in the *BPS Direct* case sued the defendant owners of Bass Pro Shops and Cabella's, alleging that "[s]ession replay code is capable of capturing nearly every action taken by a website visitor while they are on the website" and can "aggregate and store website users' data" across all of the sites they monitor to potentially "match the fingerprint with the user identity." *Id*. at *2-*3. Bass and Cabela's Privacy Policy and Terms of Use advising of the data collection were located "on the homepages of their websites in smaller low-contrasting font at the bottom of the webpages" and "do not prompt website visitors to agree to or view the Privacy Policy or Terms of Use during their website visit." *Id*. at *1.

The *BPS Direct* court found that the plaintiffs whose sensitive personal information was not disclosed lacked standing and dismissed those claims with prejudice. *Id*. at *6. The court held, "[w]e find Website Users who did not disclose highly sensitive personal information such as medical diagnosis information or financial data from banks or credit cards cannot establish concrete harm." *Id*. In other words, plaintiffs' allegations that the session replay *can* collect personal data is insufficient if they did not, in fact, do so for those plaintiffs. *See id*. at *6, *16

The *BPS Direct* court also explicitly ***rejected*** the reasoning and holding of *James v. Walt Disney Co*., 2023 WL 7392285, at *7 (N.D. Cal. Nov. 8, 2023)[2], also cited by Plaintiff Pacana, because it pre-dated the U.S. Supreme Court's decision in *TransUnion*, which clarified the requirements for Article III standing. As the *BPS Direct* court explained, "[w]e disagree with Judge Chen's reasoning to the extent it suggests viewing activity, search activity, and purchase behavior is enough to establish concrete harm. **Judge Chen relied on precedent set by the Court of Appeals for the Ninth Circuit before it had the benefit of the Supreme Court's guidance in *TransUnion*. We are guided instead by the law of standing following *TransUnion*.**" *Id*. at *14 (emphasis added) (citations omitted).

In her briefing and during oral argument before this Court, Plaintiff relied heavily upon another case that pre-dated *TransUnion* by six years: *In re Google Inc. Cookie Placement Consumer Priv. Litig*., 806 F.3d 125, 132 (3d Cir. 2015). First, *Google Cookie Placement* does not apply the law of standing based on the *TransUnion* case. The *Google Cookie Placement* court stated that "the actual or threated injury required by Article III may exist solely by virtue of statutes creating legal rights, the invasion of which creates standing." *Id.* at 134. But in *Spokeo* and again in *TransUnion,* the U.S. Supreme Court later rejected the exact standing analysis used in *Google*

[2] *Motion to certify appeal denied*, 2024 WL 664811 (N.D. Cal. Feb. 16, 2024).

Cookie Placement: "As the Court emphasized in *Spokeo*, 'Article III standing requires a concrete injury even in the context of a statutory violation.'" *TransUnion*, 594 U.S. at 426 (quoting *Spokeo*, 578 U.S. at 341). Simply put, the analysis of the *Google Cookie Placement* case is not in line with modern U.S. Supreme Court law on standing as set forth in *TransUnion*.

Second, the *Google Cookie Placement* case is also distinguishable because it involved defendants creating code to circumvent the settings on users' browsers and placing third-party cookies on their browsers ***even after the users had activated cookie blockers***. *Id.* The consumers in that case arguably had an expectation of privacy because they had enacted cookie blockers. Those circumstances are not alleged or present here. Plaintiff has not alleged that she had activated cookie blockers or that Vivint used code to circumvent the browser settings. Plaintiff's reliance on the *Google Cookie Placement* case is not persuasive or on point.

Likewise, Plaintiff's reliance on California cases, including her counsel's own pending litigation in California, *McClung v. AddShopper, Inc*., 2024 WL 189006 (N.D. Ca. Jan. 17, 2024), is equally inapplicable. In her arguments, Plaintiff conflates the roles of AddShoppers with that of the retailers, including Vivint. Citing *McClung*, Plaintiff argues that ***AddShoppers*** "[m]isappropriates a person's browsing activity across a network of thousands of online retailers and uses it to barrage the person's devices with unwanted email communications (particularly without giving the person a way to put a stop to the communications)," which, she argues, "adequately allege[s] 'the type of intrusion of privacy and seclusion that can be vindicated in federal courts.'" Response at p. 9 (citing *McClung*, 2024 WL 189006, at *1). But the quoted analysis in *McClung* concerned standing against ***AddShoppers*** – not the retailers. *See id*. at *1-*2. Even the California district court in *McClung* acknowledged that "standing is a close question" for the retailer defendants. *Id*. at *2. And, further, this is merely a long-winded version of the same

reasoning that the *Cook* court **rejected** as "circular reasoning [that] simply folds back onto a bare statutory violation, which the Supreme Court has clarified cannot be the basis for standing." *Cook*, 689 F. Supp. 3d at 64 (citing *TransUnion*, 549 U.S. at 424).

Even if this Court were to consider California decisions in its analysis, many other cases support dismissal of this case for lack of standing. *See e.g., Lightoller v. Jetblue Airways Corp*., 2023 WL 3963823, at *4 (S.D. Cal. June 12, 2023) (finding no concrete harm where "the only internet communications specifically alleged in the complaint is that Plaintiff 'obtain[ed] information on flight pricing'" which "is not personal information"); *Byars v. Sterling Jewelers, Inc.*, 2023 WL 2996686, at *3 (C.D. Cal. Apr. 5, 2023) ("Plaintiff does not allege that she disclosed any sensitive information to Defendant, much less identify any specific personal information she disclosed that implicates a protectable privacy interest. She therefore has not identified any harm to her privacy."); *Mikulsky v. Noom, Inc.*, 682 F. Supp. 3d 855, 864-865 (S.D. Cal. 2023) (holding that plaintiff's "conclusory allegations" that she used "her mouse to hover and click on certain products and services" and typed "her personal information into text fields" were "insufficient to establish that she suffered a concrete harm"); *I.C. v. Zynga, Inc.*, 600 F. Supp. 3d 1034, 1049-50 (N.D. Cal. 2022) (finding disclosure of "basic contact information, including one's email address, phone number, or ... username" inadequate to establish standing).

Perhaps recognizing the deficiencies in her claim against Vivint and the lack of any personal, concrete harm to Ms. Pacana, Plaintiff instead refers to a broad, hypothetical scheme involving other retailers. Citing the *Google Cookie Placement* case, Plaintiff argues that "AddShoppers with retailers help runs a mass surveillance network" that captures people's "web browsing history and associates it with their personal information" creating a "dossier" on each individual. (Hearing Transcript 09/13/2024, at p. 34). As established above, however, the *Google*

Cookie Placement case is both legally and factually distinguishable from the present case. Plaintiff's theory also runs afoul of U.S. Supreme Court authority on Article III standing, requiring a particularized, concrete injury that affects the plaintiff in a "in a ***personal and individual way***." *Spokeo*, 578 U.S. at 338 (emphasis added). "To establish injury in fact, a plaintiff must show that he or she suffered an invasion of a legally protected interest that is concrete and particularized and actual or imminent, not conjectural or hypothetical." *Id*. Plaintiff cannot base her theory of harm on a hypothetical dossier. More importantly, it is undisputed that Vivint did not collect any highly sensitive personal or financial information for Plaintiff Pacana. Thus, to the extent *any actual* content of communications concerning Pacana was collected – which she has failed to show – it is more likely from her use of the websites of "at least a dozen companies for several years." (Complaint at ¶ 66). But it was not and cannot be connected with Vivint. Under these circumstances, Plaintiff cannot establish standing as to Vivint. *See In re BPS Direct, LLC*, 2023 WL 8458245, at *12 ("We find Website Users who did not disclose highly sensitive personal information such as medical diagnosis information or financial data from banks or credit cards cannot establish concrete harm."); *Massie*, 2022 WL 534468, at *3 (finding that "Plaintiffs do not allege that any of their information collected by the Session Replay software was personal or private within the common law understanding of a privacy right" and dismissing because "Plaintiffs have not suffered a concrete injury because they do not have a privacy interest at stake"). Plaintiff's broadly pleaded allegations fail as a matter of law.

Plaintiff Pacana cannot establish a concrete injury necessary for Article III standing against Vivint, and her claims must be dismissed as a matter of law.

II. Plaintiff fails to state a claim against Vivint under the Pennsylvania Wiretapping and Electronic Surveillance Control Act.

For similar reasons – and providing an independent basis for the complete dismissal of her claims – Plaintiff Pacana has failed to state a claim under WESCA. As established above, Plaintiff has failed to plead or demonstrate any injury or harm. Additionally, Plaintiff has failed to allege that any "contents of communication" were intercepted – as required by WESCA – because website browsing activities and keystrokes are not protected. Vivint's website provided notice in its Privacy Policy of the collection of user information, and Plaintiff had no reasonable expectation of privacy on a retail website. Additionally, Plaintiff fails to plead that the alleged interception occurred in Pennsylvania. Plaintiff Pacana's complaint should be dismissed for failure to satisfy the required elements under WESCA.

A. Plaintiff cannot show that any "contents of a communication" were intercepted by Vivint.

WESCA defines "contents" of a communication as "information concerning the substance, purport, or meaning of that communication." 18 Pa.C.S.§ 5702. "Contents" do "***not include record information regarding the characteristics of the message*** that is generated in the course of the communication." *Cook*, 689 F. Supp. 3d at 68 (emphasis added). Merely browsing a website does not constitute a "communication." *Id*.

In *Cook*, the Western District highlighted the distinction between record location information and the substantive content of a communication, rejecting the plaintiff's cursory argument that "once you're on the website, you've communicated" for purposes of WESCA. *Id.* The *Cook* plaintiff interacted with the website through cursor movements, mouse clicks, and typing in product searches; she did not enter any personal information or make a purchase. *Id.* at 70. The court held that such activity "does not plausibly reveal the substance of any communication." Rather, the activity is "routing information," and "[n]avigating through a website's multiple pages

is not the substance of a communication." *Id.* Further, the court determined that typing search terms that correspond to "different physical locations of pages, documents and files on [the website operator's] servers" is not a communication giving rise to a claim under WESCA. *Id.*

Here, Plaintiff Pacana alleges that she "visited" Vivint's website – but she does not allege that she even entered any search terms on the website, like the *Cook* plaintiff did. Ms. Pacana did not enter any personal information or purchase any items on the website.[3] First, Plaintiff's visit to the website, by itself, is insufficient to state a claim under WESCA. *Id.* at 71-72. Second, any navigation on Vivint's site during her single "visit" merely redirected her to different locations on the website with different location identifiers, or URLs. Such location identifiers "have classically been associated with non-content means of establishing communication." *Id.* at 71. "Navigating through a website's multiple pages is not the substance of a communication; it's an action taken to go to a digital location." *Id.* at 70. Ruling otherwise would result in an "expansive interpretation [that] would impermissibly render the distinction between content and non-content in the statute superfluous." *Id.* at 72. Plaintiff has not alleged sufficient facts to establish that any "contents of a communication" were captured during her "visit" to Vivint's website to satisfy the requirements of WESCA.

Plaintiff cites *Oliver v. Noom, Inc.*, 2023 WL 8600576, at *1 (W.D. Pa. Aug. 22, 2023), to argue that her website movements are "contents of a communication" under WESCA. But *Noom* highlights the very distinction between record information and substantive communications that is fatal to Plaintiff's claim. The *Noom* plaintiffs alleged that the website "'records all website visitor actions, including information typed by the website users while on the website'" and "can include names, emails, phone numbers, addresses, social security numbers, date[s] of birth, and more[.]'"

[3] Complaint at ¶ 66.

Id. *Even in those circumstances*, the court held that the "contents of communication inquiry" is "'a case-specific one' that will largely depend on surrounding facts and context," and therefore, additional discovery was required to determine whether such information was "content" in the context of that case. *Id*. at *7 (citations omitted).

By contrast here, Plaintiff Pacana does not allege that she entered any "highly personal information and substantive communications that can be linked directly to a website user's identity," like in *Noom*. *Id.* Rather, she alleged the exact opposite: **she never provided personal information to Vivint**.[4] She never entered her email address, date of birth, social security number, bank account numbers, health information, or any other personal information when using the website. She never purchased anything on the website. As *Cook* highlighted, website movements – *and even search terms, which were not entered here* – merely redirect the user to a different location on the website and do not constitute content of communications. *Cook*, 689 F.Supp.3d at 71-72. Further, Plaintiff's argument that any visit to a website suffices to satisfy WESCA would negate the need for the "case-specific" inquiry that the *Noom* court said is mandatory. *Noom*, 2023 WL 8600576, at *7.

Plaintiff also cites *Braun v. Philadelphia Inquirer, LLC*, to argue that her website visit satisfies WESCA. 2023 WL 7544160, at *1 (E.D. Pa. Nov. 13, 2023). But that case is easily distinguishable from the subject case. In *Braun*, the plaintiffs sued the Inquirer, a tabloid media organization, claiming that the website tracked the videos plaintiffs watched, listed in Uniform Resource Locators (URLs), on its website and mobile app – "thereby disclosing the titles to specific videos that Plaintiffs requested or viewed." *Id*. The URLs for the Inquirer website and app captured the titles and thereby possibly the content and subject matter of the videos. *Id*. But

[4] Complaint at ¶ 66.

the Inquirer argued that the captured URLs still did "not prove that the user actually requested or watched the video." *Id*. at *3. The court found that argument insufficient to grant the motion to dismiss at the initial pleading stage, because "the Inquirer makes arguments that rely on factual assumptions that have not been established in the factual record at this stage of litigation." *Id* at *4. Given the potential substance of the information concerning the titles of the Inquirer videos, the Court determined that whether that URL information constituted "content of a communication" for the purposes of WESCA was a fact issue requiring further investigation during discovery.

In this case, in direct contrast, Plaintiff alleges that she merely "visited" Vivint's website. Complaint at ¶ 66. She does not even allege that she entered any search terms on Vivint's website that could have been included in a URL. Further, Vivint sells home security systems. It does not promote tabloid stories, and its website does not contain content that could potentially relate to a user's personal preferences, opinions, or political beliefs. Contrary to the information captured by the Inquirer, Plaintiff Pacana alleges only that the following information was captured from her visit to Vivint's site:

vivint_com:
email campaigns:
- date entered campaign: '2023-01-24T20:49:30.860000+00:00'
last status change: '2023-01-24T20:49:30.860000+00:00'
last visit: '2023-03-10T18:45:58.213000+00:00'

Id. at ¶66. The captured information contains no substantive information whatsoever. Nor could it. Plaintiff never alleged in her Complaint that she even entered any search terms (which still would not qualify as substantive content of communications) or any other activity on Vivint's site that could have been contents of communication. *Id*. Plaintiff alleges only that she "visit[ed] [Vivint's] website on January 24, 2023," and that she "never provided personal information

(including her email) to Vivint." *Id*. She generically alleges that Vivint "carefully tracked her visit and sent back information" to AddShoppers but identifies no substantive "contents of a communication" that was captured – only the information set forth above. Unlike the cases relied upon by Plaintiff, there is no assertion that Vivint captured Plaintiff's personal information or even any allegation of what she did on her single "visit" to Vivint's website. Plaintiff's bald allegations are not sufficient to carry her WESCA claim. Ms. Pacana's simple browsing of Vivint's site, without making a purchase or even entering her email address, did not provide any contents of a communication sufficient to state a claim under WESCA. The *Braun* case is inapplicable here.

Simply put, data concerning Ms. Pacana's single visit to Vivint's website cannot form the basis of a claim under WESCA against Vivint. *See Cook*, 2023 WL 5529772, at *8 ("When a website user moves the cursor or clicks the mouse, it does not plausibly reveal the substance of any communication. . . . Navigating through a website's multiple pages is not the substance of a communication; it's an action taken to go to a digital location.").

B. Plaintiff consented to the alleged interception of her website visit.

Plaintiff's arguments concerning consent ignore both the relevant law and the facts of this case. Citing a slew of cases from California and other jurisdictions, Plaintiff complains that she did not *expressly consent* to the collection of data. But express consent is not required under WESCA. And, directly contrary to Plaintiff's arguments, "prior consent" does not require "actual knowledge." *Popa v. Harriet Carter Gifts, Inc*., 52 F.4th 121, 125 (3d Cir. 2022) ("Though Popa claims she never saw the policy, the Pennsylvania Supreme Court has said that **"prior consent" in § 5704(4) does not require "actual knowledge."**) (emphasis added) (citing *Commonwealth v. Byrd*, 661 Pa. 85, 98, 235 A.3d 311, 319 (2020)). The Pennsylvania Supreme Court has held that "our case law illustrates that 'prior consent' can be demonstrated when the person being recorded

'knew or should have known, that the conversation was being recorded.' This standard is one of a reasonable person, and not proof of the subjective knowledge of the person being recorded as Appellant advocates." *Byrd*, 235 A.3d at 319.

Thus, implied consent is sufficient to defeat a WESCA claim. "Reasonable people understand that what they do on the Internet is not completely private. How could it be?" *Farst*, 2023 WL 7179807, at *4 (citations omitted). A modern, reasonable user of the internet has no expectation of privacy when she decides to navigate to a retailer's website. That is particularly true when the information she shares with the website is simply "visiting" its pages and presumably browsing for products. Indeed, the user knows or should know *before* going onto a retailer's website that her website use is being tracked. In modern internet usage, cookies are ubiquitous, and so is data tracking. Anyone who has been on most any retail, commercial, social media, or news website knows and expects this.

As described by the court in *Farst*, an individual has no greater expectation of privacy on the internet than she would in a physical store, where her browsing activity would most certainly be observed by store clerks and perhaps recorded by a surveillance camera. Here, "[Plaintiff's] decision to visit [Vivint]'s publicly accessible website rather than its physical store did not increase [her] expectation of privacy or expose [her] to a concrete harm that otherwise did not exist." *Id.* at *6. And Plaintiff's imagined scenario – where neighboring stores collude to determine a shopper's identity and add the customer to marketing list – has no applicability here as to Vivint. Vivint did not have any information concerning Plaintiff Pacana's identity – *because she did not provide that information to Vivint*. Vivint could not have provided information to anyone to identify Plaintiff because it did not have that information itself. Plaintiff Pacana did not even receive an email from Vivint, so she was not even on its marketing list. Again, Plaintiff's broadly pleaded hypothetical

about what could have happened has no significance as to *what actually did happen*. And Plaintiff's claim must be judged on the facts, not on speculation or hyperbole.

By accessing and using Vivint's website, Plaintiff impliedly consented to the potential collection of data.

CONCLUSION

In re BPS Direct, LLC, the court highlighted the only legal issues before the court, which are almost identical to those presented against Vivint here:

> We today address website users' challenges to retailers secretly tracking consumers' keystrokes and chosen webpages while browsing the retailers' websites. We put aside the rhetoric surrounding retailer marketing efforts versus surveillance. We must focus on the legal questions of whether website users suffer concrete injury from hidden tracking depending on what the retailer learns and, if so, whether the retailers' conduct in tracking their website users' conduct violates federal and state law.

705 F. Supp. 3d 333, 340 (E.D. Pa. 2023). After "put[ting] aside the rhetoric" to focus on the probative legal questions, Plaintiff Pacana has no claim against Vivint based on her factual allegations and the applicable law. Plaintiff cannot show any concrete harm as to Vivint. As a result, she lacks Article III standing and she cannot state a claim for relief against Vivint under WESCA. For these same reasons, as well as those set forth in Vivint's previously filed briefs and in oral argument, Plaintiff Pacana's claims against Vivint should be dismissed as a matter of law. Defendant Vivint respectfully requests that the Court grant the motion to dismiss.

[SIGNATURE ON THE FOLLOWING PAGE]

Respectfully submitted,

FROST BROWN TODD LLP

/s/ Tara Hopper Rice

Tara Hopper Rice
PA I.D. #313724
Union Trust Building
501 Grant Street, Suite 800
Pittsburgh, PA 15219
trice@fbtlaw.com

Counsel for Defendant,
Vivint, Inc.

CERTIFICATE OF SERVICE

I, TARA HOPPER RICE, ESQUIRE, certify that on this date, the foregoing **VIVINT, INC.'S SUPPLEMENTAL BRIEF IN SUPPORT OF MOTION TO DISMISS** has been filed electronically, and is available for viewing and downloading from the ECF System, has been served via the Court's electronic filing service on all counsel of record, and/or was also served via USPS on the following parties who have not consented to electronic service:

Charles E. Schaffer
Levin Sedran & Berman
510 Walnut Street, Suite 500
Philadelphia, PA 19106

J. Austin Moore *(pro hac vice)*
Norman E. Siegel *(pro hac vice)*
Kasey Youngentob *(pro hac vice)*
Stueve Siegel Hanson LLP
460 Nichols Road, Suite 200
Kansas City, MO 64112

Attorneys for Plaintiffs,
Amelia Ingrao and Elisabeth Pacana

Tomio B. Narita
Womble Bond Dickinson
50 California Street, Ste 2750
San Francisco, CA 94111

Attorney for Defendant AddShoppers, Inc.

Joseph Wolfson
Stevens & Lee, P.C.
1500 Market Street
East Tower, Suite 1800
Philadelphia, PA 19102

Ari N. Rothman *(pro hac vice)*
Jane B. Baber *(pro hac vice)*
VENABLE LLP
600 Massachusetts Avenue NW
Washington, D.C. 20001

Attorneys for Defendant Nutrisystem, Inc.

Dated: October 15, 2024

By: */s/ Tara Hopper Rice*
Tara Hopper Rice